UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/812,352 | 03/29/2004 | Hirokazu Ougi | 773-005con | 2689 |

39600 7590 07/28/2005

SOFER & HAROUN LLP.
317 MADISON AVENUE, SUITE 910
NEW YORK, NY 10017

| EXAMINER | |
|---|---|
| CALLAHAN, PAUL E | |
| **ART UNIT** | **PAPER NUMBER** |
| 2137 | |

DATE MAILED: 07/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/812,352 | OUGI ET AL. | |
| | Examiner | Art Unit | |
| | Paul Callahan | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on *30 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-6,9-12 and 15-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,9-12 and 15-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 09/365,446.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) ~~Paper No(s)/Mail Date~~ _____ PC
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-6, 9-12, and 15-24 are pending and have been examined. No claim numbers 7, 8, 13, or 14 were presented in the application.

### *Claim Objections*

2. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not). No claim numbers 7, 8, 13, or 14 were presented in the application.

### *Double Patenting*

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 5, 6, and 9-12 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 7, 8, 13, and 14 of copending Application No. 09/365,446. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 7, 8, 13, and 14 claim nearly identical methods of encryption algorithm sharing and network communications methods as claims 5, 6, and 9-12 of the instant application. Claims 7, 8, 13 and 14 appear to be narrower versions of the pending claims and thus render them obvious.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by Davis (6058478). Davis presents a method of updating cryptographic information, including algorithms, in remote devices. In claims 5, 6, and 8, the most succinct description of the method, an upgrade entity generates an upgrade message (claim 5), encrypts the

message with the recipient's public key (claim 6), and sends the resulting cryptogram to the remote device. The remote device accesses the cryptogram, which anticipates use of an encryption algorithm at the remote device, authenticates the contents, and performs the upgrade (claim 5). The upgrade includes deleting a previously existing algorithm and modifying that now-deleted algorithm to update the cryptographic algorithm. As the update is now the entirety of the now-stored algorithm, it is apparent that the now-stored algorithm was sent in the upgrade message.

7. Claims 20 and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Spies et al. (RE38070). From line 43 of column 15 through line 17 of column 16, Spies et al. detail the selection of an encryption algorithm for use between two entities. This process includes obtaining the identities of the originating and receiving participants, as embodied in their encryption indices. The originating entity arrives at these values internally, and hence they come from the transmission (originating) side. The sum of these indices is shown in Table 1 , which reads on applicant's database. The table shows a correspondence between a participant and encryption algorithms available to that entity, thereby anticipating the second clause of claim 20. Spies et al. say that the parties are trying to agree on an encryption algorithm, and hence the determination step is anticipated. The implication that the originating party encrypts data indicates that notification is given that a suitable algorithm exists. With respect to claim 21 , the originating participant selects an algorithm and hence information indicating the encryption algorithm has been transmitted to the sender, albeit internally. Reception of a

decryptable message constitutes notification at the receiving participant of enabled communications.

***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 2-6, 9-12, 15-19, and 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies et al. in view of Davis.

Spies et al. present a system for encryption algorithm negotiation. A potential sender compares a list of the algorithms supported internally with a list of those supported by the intended recipient. They do not, however, plan a course of action for when different algorithms are used at the sending and receiving sides. Davis presents a method of upgrading encryption parameters in remote entities (see for example claims 5, 6, and 8). His scheme includes an upgrade entity encrypting encryption algorithms under an algorithm operable by the recipient of the encrypted algorithm, thereby upgrading the algorithm while ensuring the security of the algorithm. He also shows, in figure 3, a communication system between two entities where a third trusted party facilitates trust between the two entities. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate

Davis' algorithm update system into Spies et al.'s algorithm selection system. As both Spies et al. and Davis indicate, algorithm use is restricted by the locales of both sender and receiver, and hence it is obvious that the upgrade entity of Davis would need to know the identities of both the sender and the receiver. The sender is the only entity that can be relied upon to know both of these identities. The joint method includes either the sender or receiver getting the updated algorithm, as such, both claims 2, 18, and 23 are rendered obvious. Claim 17 is broader than claim 18, and hence is also rendered obvious.

Claim 24 represents the apparatus carrying out the method of claim 23 and is therefore rejected on the same basis as is that claim.

Davis' fifth claim teaches including signatures within the cryptogram, thus obviating claims 3 and 19, With respect to claim 4, Davis' figure 3, which shows communications flowing from the trusted entity through the sender to the receiver, renders sending the signature with the encrypted algorithm to the sender and then to the receiver obvious.

Regarding claims 5 and 11, the combination of Spies et al. and Davis has already been shown to render obvious receiving the identities of the sender and the receiver from the sender. Spies et al. show a table that reads on applicant's database. Davis' demonstration of encrypting an algorithm with an algorithm operable by the entity

that receives the encrypted algorithm meets the limitations of the last clause of claims 5 and 11.

With respect to claims 6 and 12, which place, in the cryptogram, a key that is based on the update algorithm and an original key assigned to the cryptogram's recipient, Davis talks about altering cryptographic keys in lines 18-25 of column 2. As described in lines 56-65 of column 1, key length is one possible modification. Thus it is obvious to include in the modification instructions a key that is based on an original key as well as the update algorithm. This key, in unaltered state, is stored in the table.
In regards to claims 9, 10, 15, and 16, the upgrade entity in Davis corresponds to applicant's encryption key management station. Spies et al. have also mentioned that a mutually trusted party holds the table used to select encryption algorithms (column 15, lines 57-59). Other aspects of these four claims have already been discussed. The limitations of claim 22 are met by the preceding paragraphs.

## *Conclusion*

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following US Patent document teaches features pertinent to the Applicant's disclosure.

Vanstone 6,178,507

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Caldwell, can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

7-20-2005

Paul Callahan